

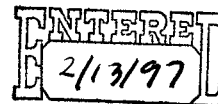


Thoroughbred Security Solutions, Ltd.

8708 Post Oak Rd.
Potomac, MD 20854-3551

February 12, 1997

Nancy Crowe
Regulatory Policy Division, Room 2705
Bureau of Export Administration, Department of Commerce
14th Street and Pennsylvania Ave., N.W.
Washington, D.C. 20230.



Dear Ms. Crowe:

Thoroughbred Security Solutions, Ltd. is a consulting company specializing in Internet/Intranet security. I've been working in the computer industry for nearly 40 years and in data security for the last twelve years. During that time, I've requested and obtained export licenses for several encryption products and know how difficult that process is.

Efforts by the US Government to limit the use and availability of strong security tools in the international data communications fields have been quite successful in the past. The cost to US businesses has been very high, however, and it is impossible to measure the wasted marketing and development resources spent tussling with questions of how to provide adequate protection for client data while not violating export regulations.

International clients have clearly stated their dissatisfaction with the strength of the 40 bit key limitations for US sourced products. Only in a few cases have I been able to satisfy their needs by obtaining specific end-user licenses for 56 bit DES based privacy products. France and some other countries have retaliated against US controls by imposing controls of their own on US imports. This places significant hardships on US companies wanting to satisfy international market needs, but unable to do so because of the export controls.

With the new Key Recovery Initiative announced by the Administration, we thought we saw a way to resolve the problem. But the Export Administration Regulations (EAR) released on December 30, 1996, fell far short of what was expected. Instead of making export of adequate privacy tools easier, it created a bureaucracy of international controls that will be extremely expensive, difficult to establish and unacceptable, for the most part, by the international clients.

The following are my observations:

- Bureau of Export Administration (BXA) controls a Trusted Third Party Facility Design, Administration, Policy and Operations. These parameters must be designed to support the most valuable keys that they may protect. But the vast majority of transactions transmitted with privacy will be of very low value. Why burden low-risk transactions with high-cost and high-overhead protection?
- International clients need privacy for their electronic transactions. Without it, they will use more traditional communications (mail, courier, private lines, etc.) They have always felt the need to be in full control of their own security. To use US technology, they must now follow the BXA regulations in using a security facility that they will not control. They must "trust" the third party to protect their

security. I don't feel that they will accept that. Particularly when equal (or better) security tools from non-US vendors will not involve a TTP!

- Most Internet transactions have very limited time-value characteristics and will not be valuable beyond a few days. The value will, in most cases, be low. Imposing a high-cost infrastructure on the users irrespective of their risk exposure will not be economically viable.
- In the event of a failure in the TTP services, the cost of recovery of the system by replacing deployed keys, smart cards, software and hardware must be borne by the customer - not the TTP. Liabilities for such additional costs - let alone any losses caused by TTP errors - probably won't be borne by the TTP - and certainly not the BXA. It is unlikely that international customers will accept this situation.
- Access to Escrowed Keys by the FBI, Interpol, the military or whomever is suspicious of the actions of one of the international customer's users, must be provided under a court order. The court having jurisdiction over the user/customer will be a function of where the user and the customer are, not the TTP. In many cases, the customer's system will be international itself. Users may be in any part of the world - and the security server in another. The complexity of international laws must be negotiated in advance of implementation of the TTP infrastructure. Bilateral agreements must be established covering all contingencies and the TTP must ascertain the validity of the order for the particular client access situation before granting access to the escrowed key. The customer must understand and accept that these arrangements are going to be properly followed in the event of a request.
- Security has always been difficult to sell. Costs of processing and key management have generally been quite high compared to the perceived risks. With the Internet giving access to the data and the reduced cost of hacking (cheap processing - well known methods - readily available talent) and the desire to transmit more valuable transactions, the risks to customers are radically higher. Thus security becomes more necessary. But they still don't want to pay much for it. To accept security, the costs must be low, the ease of use by ordinary clerks and administrators easy, and the disruption in normal business data flow minimal. The EAR's regulations will be expensive, complex to establish and disruptive to normal operations.
- Many security tools do not utilize traditional shared secret (asymmetric key) technology. Escrowed key concepts rely largely on this kind of security, and to modify public key based tools to work with this concept is not a clean situation. Session keys provide a solution that can work, but will be more difficult to recover than by using a shared secret key.
- Adding another data base of secret data increases the possibility of exposure. The BXA stipulates they be told when any Key Recovery Agent leaves the employ of the TTP. A replacement person must meet their criteria and be accepted before beginning work. But if the departing TTP employee takes a copy of the customers' secret keys with him, who is to know? Will it be necessary to redeploy all secret escrowed keys contained in the database in order to maintain the necessary level of security?

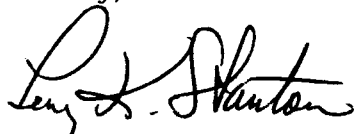
September 10, 1994

Fortunately, the EAR does make provision for customers to manage their own keys. By avoiding the TTP situation, there may be some situations where American security companies can market product internationally. Some of the regulations will still be onerous to international customers and governments. It remains to be seen if we can make it appear that these measures will provide enhanced capabilities that "improve" security products by providing protection against internal fraud and suspicious activity.

I feel that the EAR will not be helpful. It offers an open market for international security providers to sell their wares to **not only** our international customers, but **also** to domestic customers who are dealing in the global market. We have already lost domestic business to Canadian firms who have less restrictive export policies and can provide strong security for EDI transactions in the international EDI market.

I would welcome the opportunity to assist in discussions of these and other problems dealing with this subject. NIST and the Interagency Working Group on Encryption may already have all the inputs they need to deal with this problem. I cannot believe international clients will accept the Key Encryption TTP approach to provide strong security, however. A much simpler, cheaper and more appropriate solution is already knocking at their door. And it doesn't bring Big Brother with it.

Sincerely,

A handwritten signature in cursive script, appearing to read "Leroy K. Stanton".

Leroy K. Stanton, President
Thoroughbred Security Solutions, Ltd.